

硬盘数据加密系统的设计及其 FPGA 实现^{*}

苗 胜, 张新家, 曹卫兵, 张开来, 戴冠中
(西北工业大学 自动化学院, 陕西 西安 710072)

摘 要: 阐述了已研制成功的基于 FPGA 芯片的硬盘数据加密系统。采用 FPGA 设计技术, 设计了支持常用对称加密算法(DES , 3DES, AES) 和用户自主开发的各种对称加密算法的硬盘数据加密系统。实现了一种基于 FPGA 芯片的直插型硬盘数据加密卡, 其对 DES 算法的加 / 解密速度达到了 200Mbps。
关键词: 硬盘数据加密系统; DES; AES; FPGA; 直插型
中图法分类号: TP309. 7 **文献标识码:** A **文章编号:** 1001-3695(2004) 10-0217-03

Design of Hard Disk Data Encryption System and Its Implementation Using FPGA

MIAO Sheng, ZHANG Xin-jia, CAO Wei-bing, ZHANG Kai-lai, DAI Guan-zhong
(College of Automation, Northwestern Polytechnical University, Xi 'an Shanxi 710072, China)

Abstract: The design of hard disk data encryption system based on FPGA is presented. The hard disk data encryption system supports DES, 3DES, AES and other kinds of symmetry-key encryption algorithms designed by users themselves. According to the structure of the system, direct-embedded hard disk data encryption card is implemented, and its encryption speed for DES is 200Mbps.
Key words: Hard Disk Data Encryption System; DES; AES; FPGA; Direct-Embedded

根据美国计算机安全研究所(Computer Security Institute of USA) 2002 年计算机犯罪和安全调查报告, 由于笔记本电脑和个人电脑硬盘被盗而导致硬盘上的数据泄密, 已经成为人们关心的信息安全问题。针对此问题, 在以往的解决方案中, 通常采用软件加密方法予以实现, 但软件加密存在着加密速度低、降低系统性能和加密软件自身安全性等方面的问题。因此, 研究基于硬件的数据加密系统具有重要的意义。本文提出了一种适用于对称加密算法的数据流硬件加密逻辑结构, 设计与实现了基于 FPGA 芯片的直插型硬盘数据加密卡。该硬盘数据加密系统与以往的软件加密方法相比, 有着加密速度快、对用户完全透明、安全性好等特点。它支持 DES, 3DES, AES 等常用对称加密算法及用户自主开发的各种对称加密算法。

1 硬盘数据加密系统体系结构及其设计方法

我们所设计的硬盘数据加密系统的体系结构如图 1 所示。

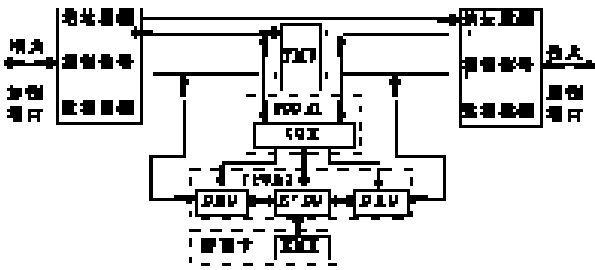


图 1 硬盘数据加密系统体系结构

- (1) TMU 临时缓存单元。其作用是存储控制信号和数据流, 并在恰当的时间将其转发, 以保证加密系统的时序完整性。
- (2) CCM 控制电路模块。本模块用来控制数据流的加 / 解密进程和加 / 解密操作, 是整个系统的神经中枢。
- (3) E / DM 加 / 解密模块。它由加 / 解密单元和两个双端口缓冲单元构成, 是实现硬盘数据加密的核心部件。
- (4) E / DU 加 / 解密单元。实现常用的对称加密算法, 包括 DES, 3DES, AES。
- (5) DMU 双端口缓冲单元。用来缓存数据, 同时把 k 组 m 位来自加密端口 / 解密端口的数据流移位转换为加 / 解密单元的一组 n ($n = k \times m$) 位待加 / 解密数据输入, 或者将加 / 解密单元的一组 n 位已加 / 解数据输出移位转换为 k 组 m 位去往解密端口 / 加密端口的数据流。
- (6) KMM 密钥管理模块。本模块负责存储和管理加 / 解密模块的密钥。在硬件结构上, 本模块是与其他模块相互分离的。

根据 FPGA 的设计流程^[6], 实现这个加密系统的整个过程可以分为以下几个阶段:

- (1) 利用 Top-down 设计方法^[7]和 Quartus 工具对核心模块进行 VHDL 描述, 然后利用 Quartus 对加 / 解密模块进行前仿真来确定所实现的加密算法程序正确性。
- (2) 利用 Synopsys 设计编译器对上面的设计进行门级综合和逻辑优化, 产生可下载到 FPGA 中的原理图或网络表。
- (3) 将网络表或原理图下载到相应的 FPGA 中, 然后对这个设计进行后仿真(时序仿真) 来最终验证 FPGA 模块设计的正确性。利用 Quartus 工具就可以完成网络表或原理图下载,

而后仿真常用的工具是 Modelsim。

(4) 利用 Protel 或 Orcad 传统设计工具设计外围电路(FPGA 配置电路、电源/时钟电路等) 的原理图,同时综合 FPGA 模块和外围电路,设计整个加密系统的原理图。最后利用 Cadence 布线工具将加密系统的原理图设计转换为印刷电路板图设计。

(5) 对试验板进行反复调试、修改、再调试过程, 最终完成硬盘数据加密系统的研制。

2 硬盘数据加密系统的FPGA 实现

依据图 1 中提出的数据流硬件加密体系结构, 我们针对计算机硬盘设计了直插型硬盘加密卡。“直插型”是相对“PCI 型”而言, 这种加密卡虽然也可以直接插入普通桌面电脑的 PCI 插槽中, 但没有定义 PCI 电气特性。

当今主流硬盘的接口界面有两种: IDE 和 SCSI。本文开发的硬盘数据加密卡是基于商业上最普及的 IDE 接口硬盘。IDE 接口的 40 个信号可划分为四大类: 硬盘读写信号; 地址信号; 16 位数据; 其他信号(上述三种信号外的所有信号)。其思路是: 将控制信号和普通数据分离开来, 即当数据线中传输的是控制信号时则直通放过, 而当数据线中传输的是普通数据时则引入加密机制, 这样就能实现硬盘的数据加密。此外, 当主机在读取硬盘参数时, 由于其参数在硬盘出厂时已经固化于硬盘内部, 所以对于这一部分数据也应当让其直通。

许多相关文献^[3~5]已经详细描述了 DES 算法的硬件实现,我们只是概述一下本文所研制的 FPGA 板卡上的 DES 算法硬件实现框架。至于其他算法的实现,与此相仿。

众所周知, DES 算法流程包括了初始置换、S 盒置换、P 盒置换、逆初始置换和一轮加/解密等基本操作。利用 VHDL 实现每一个基本操作都很简单,但是难点在于如何将这基本操作在 VHDL 中组合在一起,利用 VHDL 程序实现 16 轮循环的 DES 加/解密。DES 算法实现框架如图 2 所示。

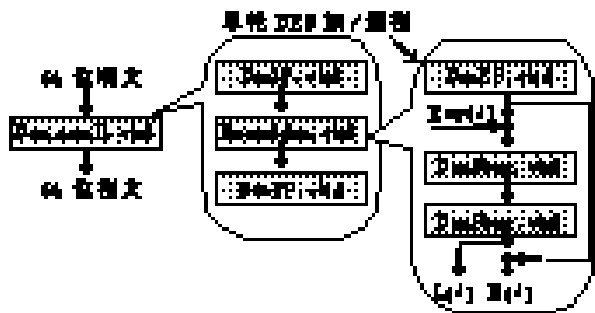


图 2 DES 算法实现框架

我们的设计思想是利用 VHDL 实现单轮 DES 加/解密这个基本操作, 然后利用组件思想将单轮 DES 加/解密操作嵌入到循环语句中, 从而实现整个 DES 算法。基于这种思想, 我们设计了七个 VHDL 文件(.vhd) 来实现 DES 算法, 这些文件之间的关系如图 2 所示。在这七个文件中, DesEP, DesSbox 和 DesPbox 是 Rounddes 的子组件。Rounddes 的功能是实现单轮 DES 加/解密操作; 进一步, DesIP, Rounddes 和 DesFP 又是 Des_small 的子组件, Des_small 的作用是实现 DES 算法的 16 轮循环。Rounddes 和 Des_small 的关键代码如图 3 和图 4 所示。通过这种两层嵌套的组件机制, 我们成功地实现了 DES 加/解密单元, 其吞吐量为 200Mbps。

外围电路包括两组驱动电路、FPGA 配置电路、电源/时钟

生成电路、智能卡接口电路、FPGA 同步和密钥扩展这六个子模块。其中密钥扩展模块与加/解密模块放在同一个 FPGA 加以实现,而原始的密钥存储在智能卡中,通过智能卡接口读入系统。用户在使用过程中,只需要将智能卡插入智能卡接口,计算机就可以正常启动运行。由于我们的加密过程是在系统的底层进行的,所以对于上层软件 and 用户来说,均是透明的。同时,由于我们采用的是硬件加密的手段,不占用系统资源,加密速度快,所以对用户在使用过程中的影响微乎其微。

<pre> Entity des _ small4 is port(...); end des _ small4; Architecture arch _des _ small of des _ small4 is - - - - - - - Component - - Declarations - - - - - component desip port(...) end component; component desfp port(...); end component; component rounddes port(...); end component </pre>	<pre> Begin - - - 16 rounds process of DES - - - Ip0: desip port map (din = > din, dout = > dataip); r _ din < = dataip when round = "0000" else r _dout; Round0 : rounddes port map (clk = > clk, reset = > reset, key = > key, din = > r _ din, dout = > dout); beforedout < = r _ dout(31 downto 0) & r _ dout(63 downto 32); Fp0: desfp portmap (din = > beforedout, dout = > dout); end arch _des _ small; </pre>
--	---

图 3 DES 算法实现的 VHDL 结构

<pre> Entity rounddes is port (...); end rounddes; Architecture behavior of des_small4 is - - - - - Component Declarations - - - - - component desep port (...); end component; component dssbox2 port(...); end component; component despbbox port(...); </pre>	<pre> Begin - - One round process of DES - rin <= din(31 downto 0); epmap: desep port map(rin, dataep) sboxin <= dataep xor key; sbmap: dssbox2 port map (sboxin, datasb); pbmap: despbbox port map (datasb, datapb) temp <= din(31 downto 0) & (datapb xor din(63 downto 32)); end behavior; </pre>
---	---

图 4 单轮 DES 的 VHDL 代码结构

3 实现结果

依照上述方案,我们将研制出的直插型硬盘数据加密板应用到计算机硬盘与 CPU 之间进行硬盘数据加密测试:

(1) 对硬盘进行分区和格式化(硬盘与 CPU 之间使用加密板),再对硬盘进行数据读写操作,测试结果如图 5 所示,数据读写完全正确,无误码情况。

(2) 在不插入智能卡或把加密板去掉, 硬盘直接和主机进行连接的情况下启动计算机。测试结果如图 6 所示, 无法找到硬盘上的操作系统和分区信息——硬盘数据被加密。

(3) 再次把加密卡插入硬盘与主机之间, 并将智能卡正确插入, 主机又可以正常启动并能看到所写入硬盘的数据, 测试结果与图 5 完全相同。

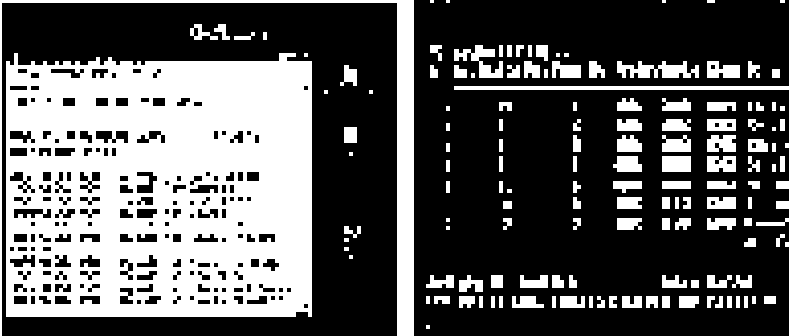


图 5 加密模块输出波形图

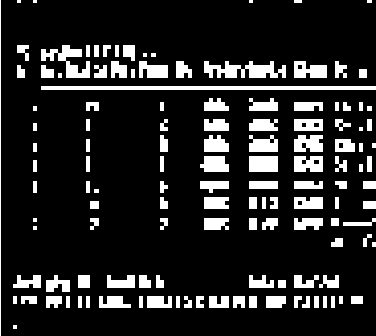


图 6 解密模块输出波形图

被测试的硬盘是昆腾火球™3228ST, 它的内部传输率和外部传输率分别为 33.3Mbps 和 16.5Mbps。我们定义:

- f_{clk1} 为 EP20K200EFC FPGA 芯片的输入频率;
- f_{co} 为晶体振荡器的输出频率, 我们将该频率二分频后输入给 f_{clk1} ;
- T_{CH} 为在 CPU 和硬盘之间传输一位数据所需要的平均时间;
- T_{CB} 为在 CPU 和 FPGA 板卡之间传输一位数据所需要的平均时间;
- $T_{E/D}$ 为在加/解密模块中加/解密一位数据所需要的平均时间;
- T_{BH} 为在 FPGA 板卡和硬盘之间传输一位数据所需要的平均时间;
- Thp_0 为插入加密卡之前, 被测硬盘在某个工作模式下的数据吞吐量(为预定值);
- Thp_B 为插入加密卡之后, 被测硬盘在某个工作模式下的数据吞吐量;
- $Thp_{E/D}$ 为 FPGA 板卡上加/解密模块的数据吞吐量;
- η_B 为 FPGA 板卡数据吞吐量之效率;

①在时钟电路中, 我们将 f_{co} 二分频后输入给 f_{clk1} , 即 $f_{clk1} = 0.5 f_{co}$;

②在某个工作模式下 Thp_0 为一个预定值, 如在 PIO_4 模式下 $Thp_0 = 132.8Mbps$, 因此: $T_{CH} = 1/Thp_0$;

③以 CPU 为参照物, 插入的加密卡相当于插入加密卡前的硬盘, 则 $T_{CB} = T_{CH}$;

④以 DES 算法为例, 其加密分组长度为 64 位, 每次加/解密需要 16 轮, 每轮需要一个 FPGA 时钟周期, 即 $1/f_{clk1}$ 。所以 $Thp_{E/D} = 64/16 \times f_{clk1} = 2f_{co} T_{E/D} = 1/Thp_{E/D} = 1/2f_{co}$;

⑤ T_{BH} 是控制模块中的信号发生电路产生的, 其值为固定值 $1/2f_{co}$;

⑥把硬盘加密卡应用到测试实验中, 可得出如下公式:

$$Thp_B = \frac{1}{T_{CB} + T_{E/D} + T_{BH}} = \frac{1}{T_{CH} + \frac{1}{f_{co}}} = \frac{Thp_0 \cdot f_{co}}{Thp_0 + f_{co}}$$
$$\eta_B = \frac{Thp_B}{Thp_0} = \frac{f_{co}}{f_{co} + Thp_0} Thp_{E/D} = 2f_{co}$$

分析以上公式, 我们可以很容易地得出: 当 Thp_0 是一个常量(预定值)时, f_{co} 是影响硬盘加密卡性能的关键参数。如果 f_{co} 增加, Thp_B , η_B , $Thp_{E/D}$, $\eta_{E/D}$ 也会相应地增加, 这样整个板卡的性能也随之改善。在实际测试中, 我们所使用的晶振的输出频率 f_{co} 为 100MHz, 也就是说 EP20K200EFC 的输入频率 f_{clk1} 为 50MHz。根据这些公式和 $Max-f_{co}$, 我们画出 Thp_B 性能曲线, 并列出了 Thp_B , η_B , $Thp_{E/D}$ 在五个工作模式下的性能参数值, 如图 7 和表 1 所示。

表 1 不同工作模式下各项参数对比

mode	Pio_0	Pio_1	Pio_2	Pio_3	Pio_4
$f_{co} = 120$					
Thp_0 (Mbps)	26.4	41.6	66.4	88.8	132.8
Thp_B (Mbps)	20.9	29.4	39.9	47.0	57.0
η_B (%)	79.2	70.7	60.1	52.9	42.9
$Thp_{E/D}$ (Mbps)	200	200	200	200	200

总体上来看, 我们研制的 FPGA 板卡已经成功加密了测试硬盘。在整个加密测试实验中, 硬盘与主机之间的传输没有可察觉的传输延迟和滞后感。

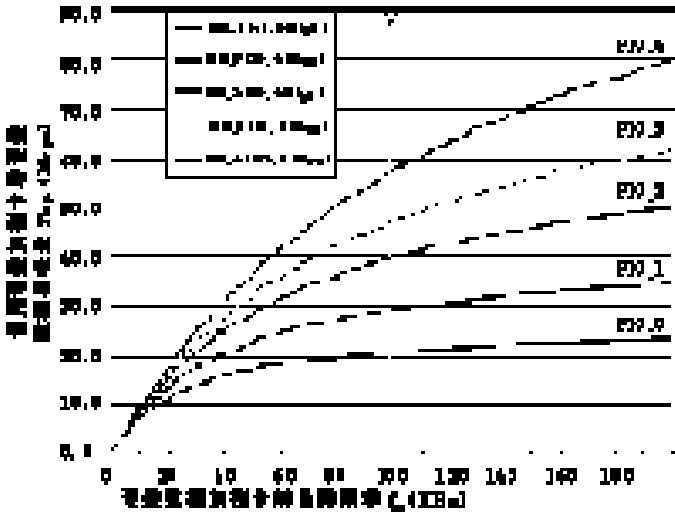


图 7 硬盘加密卡工作效率

4 结论

(1) 测试结果表明, 我们已成功开发出一种基于 FPGA 芯片的直插型硬盘加密卡。该加密卡对 DES 算法的加密速率为 200Mbps, 符合计算机硬盘数据加密的要求。

(2) 在这种加密机制下, 硬盘上的操作系统和用户数据一起被加密, 破解者误认为是一块没有被格式化的空盘, 信息隐藏级别高。同时, 由于操作系统被加密, 因此加密卡对操作系统是透明的, 支持多操作系统下的 IDE 硬盘数据加密。

(3) 这种数据流硬加密体系结构具有良好的可扩展性, 它可以升级并应用到不同的数据安全传输领域。

参考文献:

[1] eck H, et al. Cipher System: the Protection of Communication[M] . London Northwood, 1983.

[2] Mayer C H, et al. Cryptography: A New Dimension in Computer Data Security[M] . John Wiley, 1987.

[3] Cameron Patterson. High Performance DES Encryption in Virtex™ FPGAS Using JBits™[J] . IEEE, 2000, 0-7695-0871-5: 113-121.

[4] K Wong, et al. A Single-chip FPGA Implementation of the Data Encryption Standard (DES) Algorithm[J] . IEEE, 1998, 0-7803-4984-9: 827-832.

[5] Teo Pock Chueng, et al. Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD[J] . IEEE, 2000, 0-7803-6355-8: III-17-III-21.

[6] 时宏伟. FPGA 技术在工程中的应用[J] . 电讯技术, 1995, 35 (4) : 33-39.

[7] 侯伯亨. VHDL 硬件描述语言与数字逻辑设计[M] . 西安: 西安电子科技大学出版社, 1999.

[8] Friedhelm Schmidt. SCSI 总线和 IDE 接口: 协议、应用和编程(第二版)[M] . 北京: 中国电力出版社, 2001.

作者简介:

苗胜(1977-), 男, 陕西咸阳人, 博士生, 主要研究方向为网络信息安全; 张新家(1961-), 男, 湖北洪湖人, 副教授, 博士, 主要研究方向为软件体系结构、网络信息安全; 戴冠中(1937-), 男, 上海人, 教授, 博士生导师, 主要研究方向为网络信息安全、自动控制等。